



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

[Handwritten signature]

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,535	12/14/2001	Barbir Abdulkader	08888512US	3243
26123	7590	05/05/2005	EXAMINER	
BORDEN LADNER GERVAIS LLP WORLD EXCHANGE PLAZA 100 QUEEN STREET SUITE 1100 OTTAWA, ON K1P 1J9 CANADA			LEMMA, SAMSON B	
		ART UNIT		PAPER NUMBER
		2132		
DATE MAILED: 05/05/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/014,535	ABDULKADER, BARBIR	
Examiner		Art Unit	
Samson B. Lemma		2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 14 December 2001.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-10 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-10 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____.

DETAILED ACTION

1. Claims 1-10 have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-5 and 10 are rejected under 35 U.S.C. 102(b) as being anticipated by

Akihiro Maebara (hereinafter referred as Maebara) (European Publication: EP

0720328A1)(Publication date: 07/03/1996)

5. As per claim 1 and 10, Maebara discloses an encryption system [Figure 1, ref.Num "2"; Abstract; column 3, lines 27-29; figure 6, ref. Num "2"] (the system has an enciphering/encryption means for enciphering an output signal of the random-number adding means] comprising:

• A transmitting device for modulating/enciphering data with a pseudo-random signal for signaling over a transmission medium; [Abstract; figure 1; column 3, lines 36-47] (The transmitting device comprises random-number generating means for generating a random-number α and a bit-adding means for adding a random-number bit generated by random-number generating means and the enciphering/encryption section enciphers the signal (DA, α) and output the ciphered signals, $(DA, \alpha)'$) and

• A receiving device for receiving said data by removing said pseudo-random signal. [figure 2, ref. Num "11"; Abstract, see the last four lines] (A receiving device deciphers the ciphered signals (DA, α) and reproduces the data DA by removing the random number bit α)

6. As per claim 2, Maebara discloses an encryption system as applied to claim 1 above. Furthermore Maebara discloses the system wherein said transmitting device [figure 1] further comprises: means to generate a second modulated signal; [figure 1, ref. 5, Num "α "] (The second modulated signal as explained on claim 4 is a pseudo-random signal and Maebara discloses as shown on figure 1, ref. Num "5" and ref. Num "α " that the second modulated signal "α " is generated by the random-number generator as shown on figure 1, ref. Num "5")

• Means to add said second modulated signal [Figure 1, ref. Num "α "] to said data signal [figure 1, ref. Num "DA"] to produce a transmitted signal; [Figure 1, ref. Num "DA, α "] and means to send said transmitted signal over a transmission medium [Figure 1, ref. Num "(DA, α) ' "].

7. As per claim 3, Maebara discloses an encryption system as applied to claim 2 above. Furthermore Maebara discloses the system wherein said receiving device [figure 2] further comprises means to generate a third modulated signal; [figure 2, ref. Num "DA, α "] (The third modulated signal as explained on claim 4 is a pseudo-random signal and Maebara discloses as shown on figure 2, the third modulated signal "α " is generated at the receiving device by decrypting the enciphered (DA,α)' using the key) and to subtract said third modulated signal [figure 2, ref. Num 11 and "α "] from said transmitted signal [figure 2, ref. Num "DA, α "] to produce a data output signal; and

means to demodulate said output signal to produce a second data output signal.[figure 2, ref. Num "DA"]

8. As per claim 4, Maebara discloses an encryption system as applied to claim 3 above. Furthermore Maebara discloses the system wherein said second modulated signal [Figure 1, ref. Num "α"] and said third modulated signal [figure 2, ref. Num "α"] are pseudo-random [figure 1, ref. Num "5"] and opposite in amplitude, but otherwise identical in phase and frequency, thereby simplifying the demodulation of said data. [figure 2] (They are inherently identical otherwise the demodulation of said data would not have been possible.)

9. As per claim 5, Maebara discloses an encryption system as applied to claim 4 above. Furthermore Maebara discloses the system wherein the parameters defining the phase, amplitude and frequency of said second modulated signal and said third modulated signal are derived from a random number generator seeded with a key, thereby increasing the difficulty of an intruder planning to intercept said transmitted signal. [See figure 1 and figure 2 and the reference "Key"].

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akihiro Maebara (hereinafter referred as Maebara) (European Publication: EP 0720328)(Publication date: 07/03/1996) in view Thomlinson et al. (hereinafter referred to as Thomlinson) (U.S. Patent No. 5,778,069)

12. As per claim 6, Maebara discloses an encryption system as applied to claim 3 above. Furthermore Maebara discloses the system wherein said second modulated signal [Figure 1 ref. Num "α"] and said third modulated signal [figure 2, ref. Num "α"] are identical. Furthermore Maebara discloses that the transmitter and receiver are seeded with the same key so that parameters derived from both are the same and when applied to said means for generating said second modulated signal and said means for generating said third modulated signal result in the same signal being generated, thereby ensuring correct reception of said transmitted signal. [see figure 1 and figure 2 and the abstract]

Although, Maebara has mentioned the random number generator at the transmitter side, the reference, does not clearly express:

That the random number generator is implemented at both the transmitter and receiver and seeded with the same key.

However, in the field of endeavor Thomlinson, discloses the random number generator is implemented at both the transmitter and receiver and seeded with the same key.[See for example figure 1, prior art].

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of implementing the random number generator at both the transmitter and receiver and seeded with the same key as per teachings of Thomlinson in to the method as taught by Maebara, in order to add the advantages of stream cipher cryptography in to the system and make the system more secure. [See Thomlinson column 3, last two lines.]

13. As per claims 7, the combination of Maebara and Thomlinson discloses an encryption system as applied to claim 6 above. Furthermore Thomlinson discloses the system wherein the data is manipulated as a 'group of bits' and the number of bits in a 'group of bits' is a parameter and may be varied for each 'group of bits'. [Column 3, last two lines; figure 1] (Stream cipher encrypts and decrypts a group of bits at a time and this meets the recitation of this claim).

14. As per claims 8-9, the combination of Maebara and Thomlinson discloses an encryption system as applied to claim 7 above. Furthermore Thomlinson discloses the

system wherein said number of bits parameter is derived from a second random number generator. [See figure 1]

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S-L.

04/28/2005


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100